

IC・ID カードの相互運用可能性の向上に係る基礎調査 概要

2007年3月28日

セコム(株)IS研究所

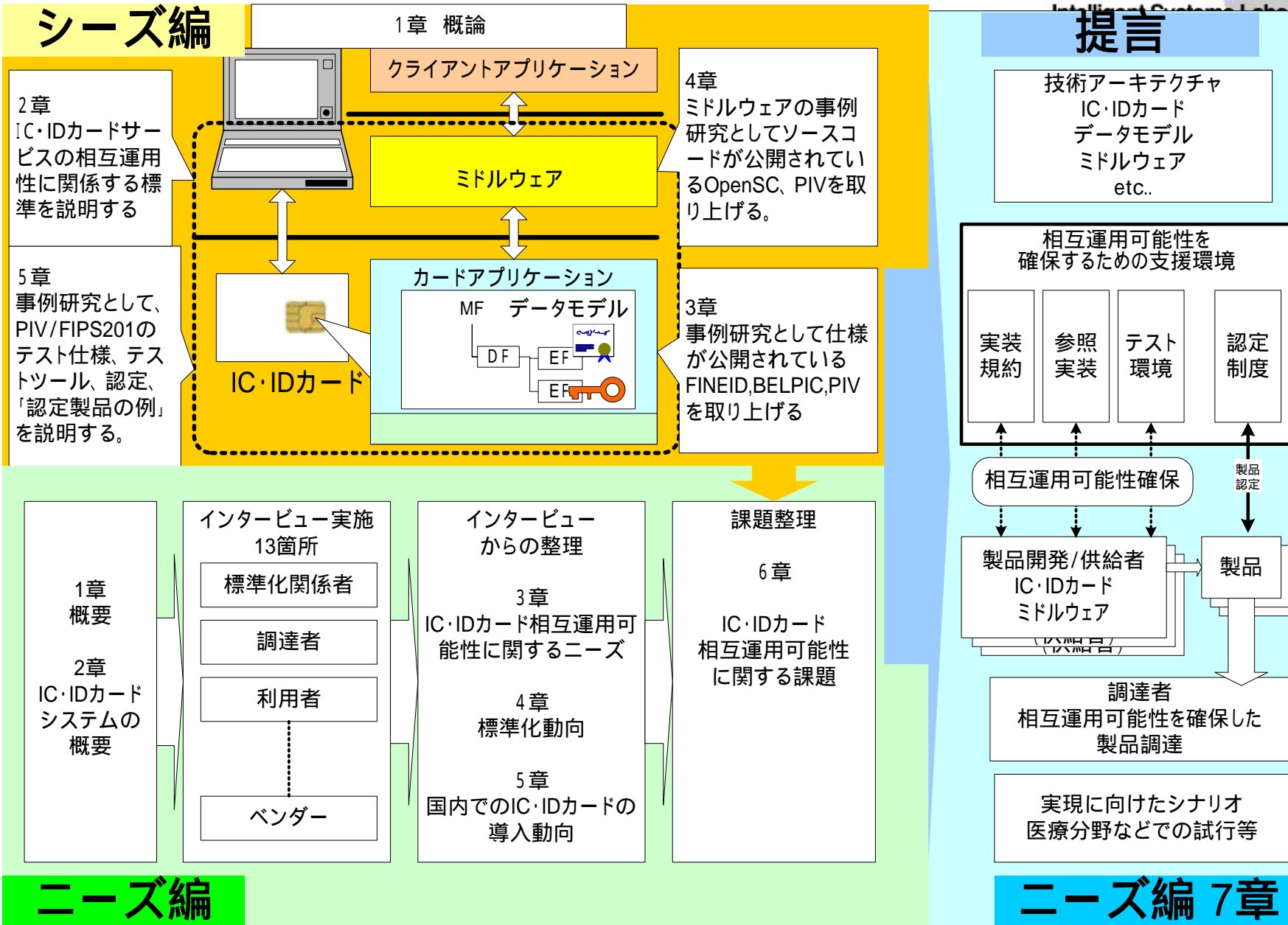
PKI相互運用技術WGリーダー

松本 泰

「IC・ID カードの相互運用可能性」 技術セミナー

- NPO JNSAでは、昨年、(独)情報処理推進機構 (IPA)の公募事業である「IC・IDカードの相互運用可能性向上に係る基礎調査」の採択を受けて実施しました。
- この調査は、シーズ調査とニーズ調査からなり、シーズ調査では相互運用可能性を実現する標準化動向や海外の取組みにおける技術体系の事例を、またニーズ調査では現在のIC・IDカードにおける相互運用可能性の実態と今後への展望を調査し、今後国内でIC・IDカードの相互運用可能性の向上に必要な、国際標準を活用した関連技術の標準化やツール開発、普及方策を提案しています。
- 調査結果については、今年の1月11日よりIPAのサイトで調査報告書が公開されています。今回の「IC・ID カードの相互運用可能性」技術セミナーでは、この調査報告書の内容を中心に、IC・ID カードの技術とその課題をご紹介します。

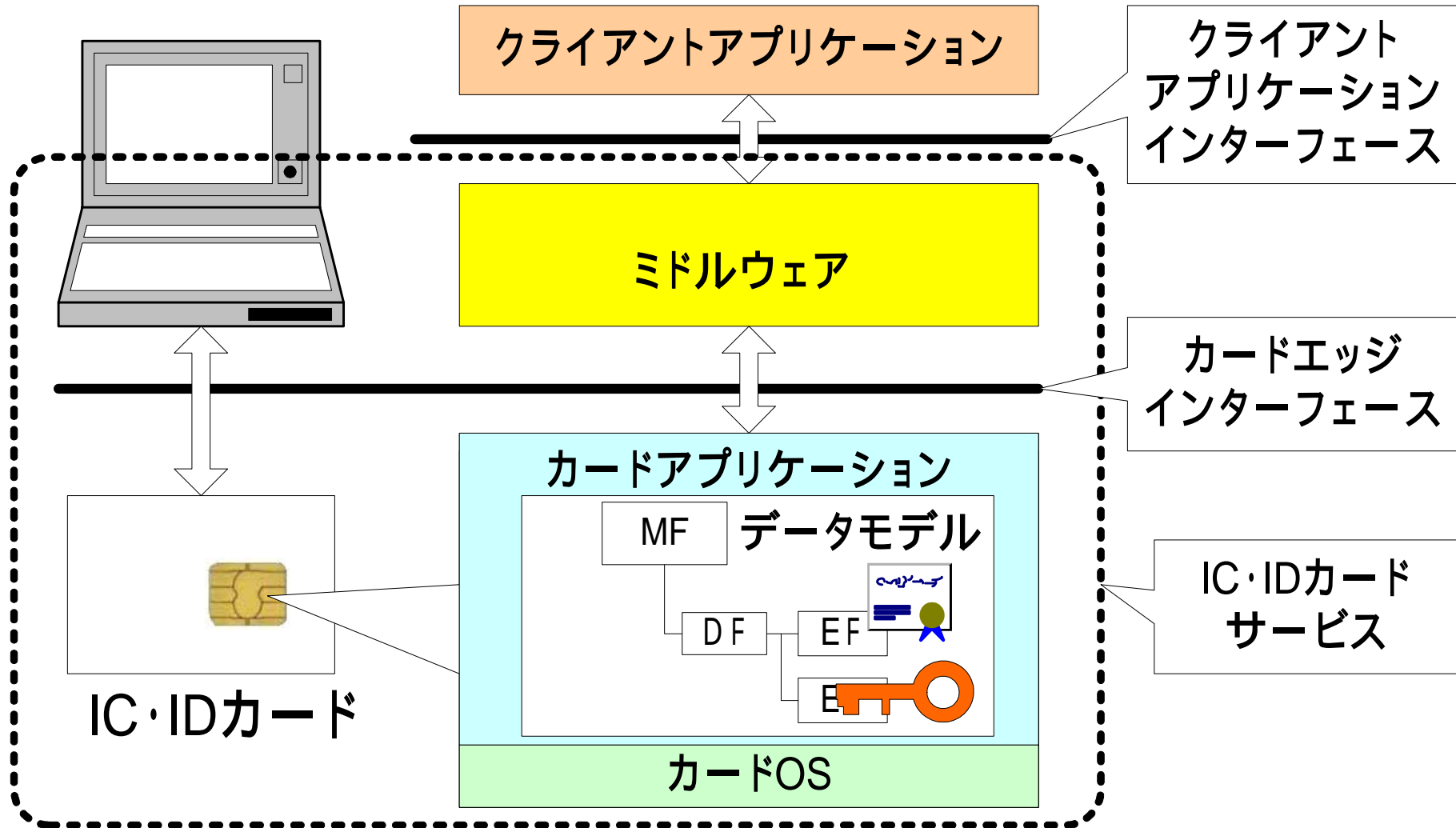
調査の全体概要



ニーズ編

ニーズ編 7章

基本的な用語



基本的な用語

| 用語 | 意味 |
|-----------------|---|
| IC・IDカード | ICカードを使った電子署名やリモート認証が利用可能なIDカード |
| カードアプリケーション | ICカード上のアプレット、データ |
| ミドルウェア | IC・IDカードを扱うための端末上のミドルウェア |
| IC・IDカードサービス | IC・IDカードとミドルウェア |
| カードエッジ・インターフェース | IC・IDカードとミドルウェア間の論理的なコマンドインターフェース APDU(アプリケーションプロトコルのデータ・ユニット) |
| データモデル | ICカード上のファイル構造、データ構造 |

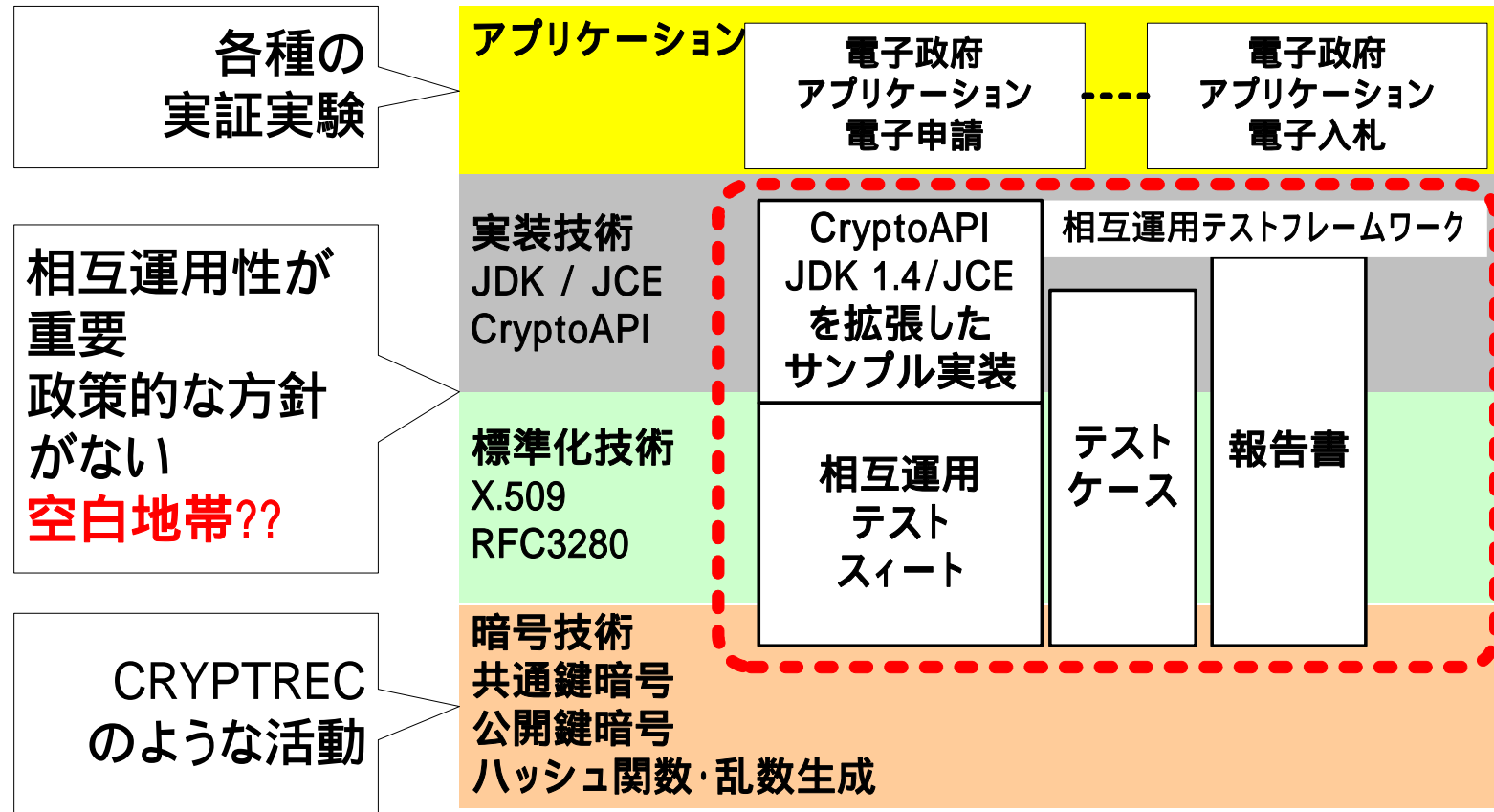
本日のメニュー

- 13:15 - 13:25
IC・ID カードの相互運用可能性の向上に係る基礎調査の概要
セコム(株) IS研究所 / PKI相互運用技術WGリーダー
- 13:30 - 13:10
ニーズ編 みずほ情報総研(株) 出口 太郎
- 13:15 - 14:55
シーズ編 セコム(株) IS研究所 / PKI相互運用技術WGリーダー
- 14:55 - 15:10
休息
- 15:10 - 15:50
シーズ編 オープンソースのミドルウェア OpenSC
(有)ロボック 伊藤 大輔
- 15:55 - 16:45
パネルディスカッション「何がICカードの相互運用可能性の問題なのか」
モデレータ JNSA研究員 / 株式会社ディアイティ 安田 直義 氏
パネラー
 - 富士ゼロックス(株) 稲田 龍 氏
 - (社)日本ネットワークインフォメーションセンター 木村 泰司
 - セコム(株) IS研究所 松本 泰
 - みずほ情報総研(株) 出口 太郎

NPO JNSAのChallenge PKIプロジェクト

Challenge PKIプロジェクトの活動 プロジェクトの目標と課題

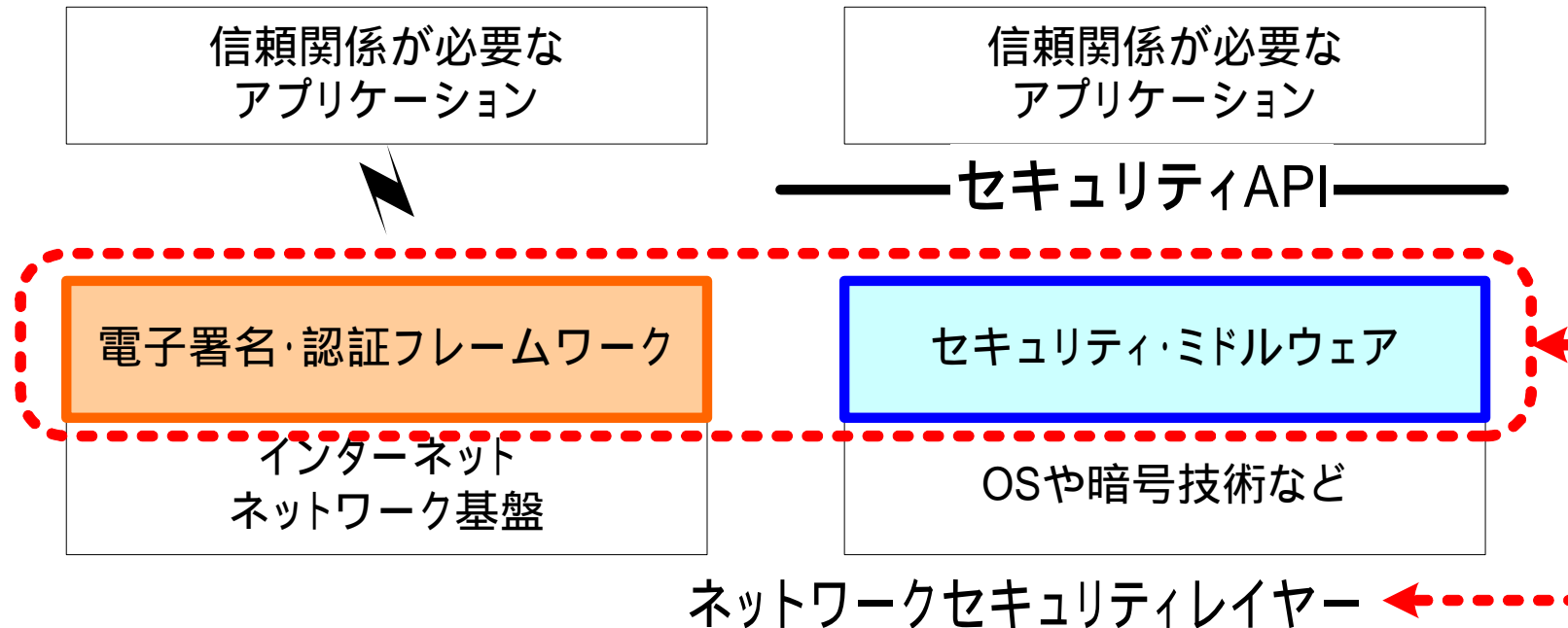
Challenge PKI 2002



複雑さを隠蔽するためどんどん階層化されていく。。
このことが、問題の本質を分かり辛くしている！！

Challenge PKIプロジェクトの活動

セキュリティフレームワークやミドルウェア重要性 *Challenge PKI 2003*



•何処でも、何時でも、誰にでもつながるユビキタスネットワークにおいて信頼の拠りどころが求められる。。。。

•ネットワーク上の信頼を実現するセキュリティ・レイヤーの必然性

•これらは、古典的なOSI参照モデルなどでは説明がつかない。。。

Challenge PKIプロジェクトの活動

セキュリティフレームワークやミドルウェア重要性 *Challenge PKI 2003*

標準化、相互運用の課題

非常に複雑なセキュリティ
プロトコルの要求

セキュリティに対応し切
れていない標準化 & 標
準化組織

テスト環境、テストケー
ス、相互運用テストが非
常に重要だが、整備が
できていない

信頼関係が必要な
アプリケーション

——セキュリティAPI——

セキュリティ・
ミドルウェア

OS

実装上の課題

暗号技術等、基礎技術が、
セキュリティ・フレームワ
ーク & ミドルウェアに組み込
まれていかない
(日本の話し。。。)

多くのバグが内在する可能性
(OpenSSLなどは典型的)

標準と実装のギャップ。何がどこま
で正しく実装されているのか分から
ない。

複雑さを隠蔽するために、どんどん階
層化されていく。そのことにより本質的
な問題点も隠蔽されていく??

複雑さと問題点が集約されていく